## What is claimed is

- 1 1. A method for managing a network, comprising the steps of:
- 2 detecting occurrence of a network event, said network event having associated
- 3 with it a network condition comprising at least one of an unplanned macro-event and a
- 4 planned macro-event related to at least one of a network element and a communication
- 5 link of said network;
- 6 classifying said network event as being at least one of a network element failure,
- 7 a communications link failure, and a security breach; and
- 8 identifying said network event as a network degradation event in response to at
- 9 least one network event exceeding a network degradation threshold.
- 1 2. The method of claim 1, further comprising the step of:
- 2 sending an alert to normalize said network degradation event.
- 1 3. The method of claim 1, wherein said network event is associated with at least
- 2 one of a network management system, a security management system, and a system
- 3 timer.
- 1 4. The method of claim 1, wherein said step of identifying comprises the step of:
- defining said network degradation event as a brink of failure (BOF) event in an
- 3 instance where said event is at least one of a type determined to cause a failure of at
- 4 least one network element within a predetermined time interval, to affect at least one of
- 5 a critically defined network functionality, and to affect a number of end users exceeding
- 6 a predetermined threshold level.
- 1 5. The method of claim 4, wherein said step of identifying said network
- 2 degradation event comprises the step of:
- assessing at least one of failure rates, mean-time-between-failures (MTBF),
- 4 mean-time-to-repair (MTTR), and spare parts availability for at least one of network
- 5 elements and communication links associated with said network event.
- 1 6. The method of claim 1, wherein in response to the step of classifying said
- 2 network event, said method further comprises the steps of:
- 3 updating an existing conditions database with indicia of said network event;

- 4 determining a latest network topology associated with said network event; and
- 5 updating a network topology database with said latest network topology.
- 1 7. The method of claim 4, wherein said step of identifying further comprises the
- 2 step of:
- 3 defining said network degradation event as a breach-of-security (BOS) event in
- 4 an instance where said network event exploits a security vulnerability resulting in at
- 5 least one of an unauthorized access, an unauthorized modification or compromise, a
- 6 denial of access to information, a denial of access to network monitoring capability, and
- 7 a denial of access to network control capability.
- 1 8. The method of claim 7, wherein said step of defining said network degradation
- 2 event as a brink-of-failure (BOF) event further comprises the step of:
- 3 correlating network events stored in said existing conditions database with
- 4 information stored in said network topology database and events stored in a scheduled
- 5 events database.
- 1 9. The method of claim 8 further comprising the steps of:
- determining whether said BOF event also causes a BOS event;
- determining whether said BOS event also causes a BOF; and
- 4 reporting at least one of said BOF event and BOS event.
- 1 10. The method of claim 9 further comprising the steps of:
- 2 categorizing said BOF event;
- 3 determining at least one corrective action procedure associated with said BOF
- 4 event; and
- 5 reporting at least one of a network element and a communications link
- 6 associated with said BOF event, and said at least one corrective action procedure.
- 1 11. The method of claim 10, wherein said step of determining at least one corrective
- 2 action procedure comprises the step of assessing a BOF database comprising historical
- 3 information associated with global network reliability practices.
- 1 12. The method of claim 9, wherein in an instance where said network degradation
- 2 event is associated with a breach-of security event, said method further comprises the
- 3 steps of:

4	categorizing	said	breach	of	security	event.
•	Categorizing	saiu	UlCacii	OΙ	SCCULITY	CVCIII,

- 5 determining at least one corrective action procedure associated with said breach
- 6 of security event; and
- displaying at least one of a network element and a communications link
- 8 associated with said breach-of security event, and said at least one corrective action
- 9 procedure.
- 1 13. The method of claim 12, wherein said step of determining at least one corrective
- 2 action procedure comprises the step of assessing a Security Vulnerabilities and
- 3 Procedures database comprising at least one of historical information of said
- 4 network and associated global security vulnerabilities and procedures.
- 1 14. The method of claim 1, wherein said step of identifying a network event
- 2 comprises the step of identifying events associated with at least one of end-user
- data traffic, in-band control traffic, out-of-band control traffic, in-band network
- 4 management traffic, and out-of-band network management traffic.
- 1 15. The method of claim 9 further comprising the steps of:
- 2 initiating a new network event upon resolving said network degradation event;
- 3 removing said network degradation event from said existing conditions
- 4 database; and
- 5 reporting said network degradation event as a resolved event.
- 1 16. The method of claim 15, wherein resolving said network degradation event further
- 2 comprises the step of at least one of:
- 3 resolving said BOF event, such that the BOF event and a BOS condition are
- 4 cleared; and
- 5 resolving said BOS event, such that the BOS event and a BOF condition are
- 6 cleared.
- 1 17. A method for managing a network, comprising the steps of:
- 2 detecting occurrence of a network event, said network event having associated
- 3 with it a network condition comprising at least one of an unplanned macro-event and a
- 4 planned macro-event related to at least one of a network element and a communication
- 5 link of said network;

- 6 classifying said network event as being at least one of a network element failure,
- 7 a communications link failure, and a security breach;
- 8 identifying said network event as a network degradation event in response to at
- 9 least one network event exceeding a network degradation threshold by defining said
- 10 network degradation event as a brink of failure (BOF) event in an instance where said
- 11 event is at least one of a type determined to cause a failure of at least one network
- 12 element within a predetermined time interval, to affect at least one of a critically defined
- 13 network functionality, and to affect a number of end users exceeding a predetermined
- 14 threshold level; and
- sending an alert to normalize said network degradation event.
- 1 18. The method of claim 17, wherein said step of identifying further comprises the
- 2 step of:
- defining said network degradation event as a breach-of-security (BOS) event in
- 4 an instance where said network event exploits a security vulnerability resulting in at
- 5 least one of an unauthorized access, an unauthorized modification or compromise, a
- 6 denial of access to information, a denial of access to network monitoring capability, and
- 7 a denial of access to network control capability.
- 1 19. The method of claim 18, wherein in response to the step of classifying said
- 2 network event, said method further comprises the steps of:
- 3 updating an existing conditions database with indicia of said network event;
- 4 determining a latest network topology associated with said network event; and
- 5 updating a network topology database with said latest network topology.
- 1 20. The method of claim 19 further comprising the steps of:
- determining whether said BOF event also causes a BOS event;
- determining whether said BOS event also causes a BOF; and
- 4 reporting at least one of said BOF event and BOS event.
- 1 21. The method of claim 20 further comprising the steps of:
- 2 categorizing said BOF event;
- 3 determining at least one corrective action procedure associated with said BOF
- 4 event; and

- reporting at least one of a network element and a communications link
  associated with said BOF event, and said at least one corrective action procedure.
- 1 22. The method of claim 20, wherein in an instance where said network degradation
- 2 event is associated with a breach-of security event, said method further comprises the
- 3 steps of:
- 4 categorizing said breach of security event;
- 5 determining at least one corrective action procedure associated with said breach
- 6 of security event; and
- 7 displaying at least one of a network element and a communications link
- 8 associated with said breach-of security event, and said at least one corrective action
- 9 procedure.
- 1 23. The method of claim 19 further comprising the steps of:
- 2 initiating a new network event upon resolving said network degradation event;
- 3 removing said network degradation event from said existing conditions
- 4 database; and
- 5 reporting said network degradation event as a resolved event.
- 1 24. Apparatus for managing a network, comprising:
- 2 means for detecting occurrence of a network event, said network event having
- 3 associated with it a network condition comprising at least one of an unplanned macro-
- 4 event and a planned macro-event related to at least one of a network element and a
- 5 communication link of said network;
- 6 means for classifying said network event as being at least one of a network
- 7 element failure, a communications link failure, and a security breach; and
- 8 means for identifying said network event as a network degradation event in
- 9 response to at least one network event exceeding a network degradation threshold.
- 1 25. The apparatus of claim 24, further comprising:
- 2 means for sending an alert to normalize said network degradation event.
- 1 26. The apparatus of claim 24, wherein said means for identifying comprises:
- 2 means for defining said network degradation event as a brink of failure (BOF)
- 3 event in an instance where said event is at least one of a type determined to cause a

- 4 failure of at least one network element within a predetermined time interval, to affect at
- 5 least one of a critically defined network functionality, and to affect a number of end
- 6 users exceeding a predetermined threshold level.
- 1 27. The apparatus of claim 26, wherein said means for identifying further comprises:
- 2 means for defining said network degradation event as a breach-of-security
- 3 (BOS) event in an instance where said network event exploits a security vulnerability
- 4 resulting in at least one of an unauthorized access, an unauthorized modification or
- 5 compromise, a denial of access to information, a denial of access to network monitoring
- 6 capability, and a denial of access to network control capability.
- 1 28. The apparatus of claim 24, wherein said means for classifying further comprises:
- 2 updating an existing conditions database with indicia of said network event;
- determining a latest network topology associated with said network event; and
- 4 updating a network topology database with said latest network topology.
- 1 29. The apparatus of claim 26 further comprising:
- 2 means for determining whether said BOF event also causes a BOS event;
- means for determining whether said BOS event also causes a BOF; and
- 4 means for reporting at least one of said BOF event and BOS event.
- 1 30. The apparatus of claim 29 further comprising:
- 2 means for categorizing said BOF event;
- means for determining at least one corrective action procedure associated with
- 4 said BOF event; and
- 5 means for reporting at least one of a network element and a communications link
- 6 associated with said BOF event, and said at least one corrective action procedure.
- 1 31. The apparatus of claim 29, wherein in an instance where said network
- 2 degradation event is associated with a breach-of security event, said apparatus further
- 3 comprises:
- 4 means for categorizing said breach of security event;
- 5 means for determining at least one corrective action procedure associated with
- 6 said breach of security event; and

7	means for displaying at least one of a network element and a communications		
8			
9	procedure.		
1	32. The apparatus of claim 29 further comprising:		
2	means for initiating a new network event upon resolving said network		
3	degradation event;		
4	means for removing said network degradation event from said existing		
5 conditions database; and			
6	means for reporting said network degradation event as a resolved event.		
1	33. The apparatus of claim 32, wherein resolving said network degradation event		
2	further comprises at least one of:		
3	means for resolving said BOF event, such that the BOF event and a BOS		
4	4 condition are cleared; and		
5	means for resolving said BOS event, such that the BOS event and a BOF condition are		
6	cleared.		
1	34. A network management system for characterizing at least one network		
2	degradation event in a communications network, comprising:		
3	a processing unit having access to at least one storage device;		
4	at least a portion of said at least one storage device having a program product		
5			
6	detect occurrence of a network event, said network event having		
7	associated with it a network condition comprising at least one of an unplanned		
8	macro-event and a planned macro-event related to at least one of a network		
9	element and a communication link of said network;		
10	classify said network event as being at least one of a network element		
11	failure, a communications link failure, and a security breach; and		
12	identify said network event as a network degradation event in response to		
	identify said network event as a network degradation event in response to		